

AVIS N° 53 / 2002 du 19 décembre 2002.

N. Réf. : 10 / A / 2002 / 044

OBJET : Avant-projet de loi relatif à l'identification, au repérage, à la localisation, aux écoutes, à la prise de connaissance et à l'enregistrement de communications et télécommunications privées aux besoins des services de renseignement.

La Commission de la protection de la vie privée,

Vu l'article 22 de la Constitution;

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en particulier l'article 29;

Vu la demande d'avis du Ministre de la Justice, du 27 novembre 2002;

Vu le rapport de M. B. DE SCHUTTER,

Émet, le 19 décembre 2002, l'avis suivant :

I. INTRODUCTION :

Le 27 novembre 2002, le cabinet restreint a décidé de transmettre pour avis le présent avant-projet de loi à la Commission de la protection de la vie privée. L'avis est attendu pour le 27 décembre 2002 au plus tard.

II. OBJET DE L'AVANT-PROJET :

1. Les services fédéraux de renseignement et de sécurité sont régis par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (M.B. du 18.12.1998). Cette loi prévoit que certaines méthodes susceptibles d'être utilisées par ces services doivent être organisées par la loi. Cela a déjà été réalisé pour les "enquêtes de sécurité" et les "habilitations de sécurité" mais pas encore pour les écoutes de sécurité. Le présent avant-projet entend, dès lors, définir la base légale à cet effet. Les services de renseignement belges – contrairement à ceux des pays limitrophes – n'ont, pour l'instant, pas accès aux moyens de télécommunication.

2. C'est pourquoi le Gouvernement estime qu'une initiative permettant de procéder au repérage et à l'interception de communications et télécommunications privées est pleinement justifiée. L'ampleur de plus en plus grande que prend la criminalité organisée au niveau international exige une vigilance accrue et des méthodes d'enquête adaptées qui peuvent surtout être utilisées rapidement et avec précision. Actuellement, le recours à de telles méthodes est organisé par les seules autorités judiciaires (loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, modifiée par la loi du 10 juin 1998), ce qui peut faire perdre un temps précieux en cas d'urgence et de menace d'attentat (p. ex. terrorisme). L'accent est toutefois mis sur le caractère exceptionnel du recours à ces méthodes et sur la nécessité d'offrir des garanties suffisantes quant à la protection de la vie privée.

3. L'exposé des motifs renvoie abondamment au droit européen, notamment à l'article 8 de la CEDH et à la jurisprudence de la Cour européenne des droits de l'Homme. Ainsi il ressort clairement de l'article 8, 2^e de la CEDH et de son interprétation par la Cour que l'ingérence dans la vie privée du citoyen pour des raisons de sécurité nationale n'est possible que si elle est prévue par une loi accessible (compréhensible) et précise. L'article 22 de la Constitution accorde également la même garantie au citoyen. L'obligation de prévoir des garanties effectives et sûres ressort clairement de la jurisprudence de la Cour de Strasbourg, surtout à la suite de l'affaire Klass (1977). Ces garanties ont trait :

1. au principe d'urgence : existence d'indices sérieux que des infractions graves sont susceptibles d'être commises ou ont déjà été commises;
2. au principe de subsidiarité : absence d'autres moyens de preuve ou seulement existence de moyens de preuve sensiblement plus délicats;
3. au principe de spécificité : intervention dirigée contre une personne ou plusieurs personnes déterminées faisant partie de ou étant en contact avec un groupe spécifique (pas d'interventions exploratoires ou proactives à caractère général);
4. au principe de motivation : uniquement sur demande et autorisation motivées par écrit;
5. au principe de stricte finalité : indication de conditions précises concernant l'accès aux renseignements recueillis et le traitement de ceux-ci (délai, conservation, destruction);
6. au principe de contrôle : présence de mécanismes de contrôle indépendants permettant un contrôle permanent, efficace et objectif.

III. EXAMEN DE L'AVANT-PROJET :

A Remarques générales :

4. La Commission rappelle avec insistance que la loi du 8 décembre 1992 est applicable à l'ensemble des traitements portant sur l'enregistrement ou la conservation des données recueillies lors des différentes mesures prévues par le projet.

Le traitement de données permettant de faciliter l'identification d'une ou de plusieurs personnes physiques peut, en effet, prendre place à plusieurs moments :

- soit lors de la phase d'identification des numéros non publiés;
- soit lors de la phase de repérage de télécommunications privées;
- soit enfin lors de la phase de conservation des télécommunications faisant l'objet d'une mesure d'interception.

Les développements technologiques multiplieront les possibilités de tels traitements.

L'application de la loi du 8 décembre 1992 aux traitements de données collectées dans le cadre de l'exercice de l'action publique a pour effet :

- 1) de permettre à la personne concernée d'exercer via la Commission de la protection de la vie privée un accès indirect aux données recueillies dans le cadre des mesures prévues par le projet (art. 13);
- 2) de soumettre des traitements, en particulier aux prescrits de l'article 5 (principes de finalité et de proportionnalité) et de l'article 16 (principe de sécurité).

Dans cette matière, la Commission a déjà émis de nombreux avis (avis n° 23/1993 concernant les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées; avis n° 09/1997 concernant l'identification et le repérage de moyens de communication et de télécommunication; avis n° 34/1994 concernant la modification de la loi sur les écoutes de juin 1994; avis n° 17/1997 concernant l'obligation de collaboration des opérateurs ainsi que les avis n° 12/1999 et 01/2001 concernant certains arrêtés d'exécution).

B. Commentaire des articles.

5. Le chapitre II contient les mesures relatives à l'identification, au repérage et à la localisation des communications et télécommunications privées.

L'article 3 contient les mesures relatives à l'identification d'un abonné ou d'un utilisateur habituel d'un service de télécommunication et à la communication de ces données d'identification. Ces données peuvent uniquement être demandées dans le cadre des "missions de sécurité" (art. 7, 1°, et 11, § 1^{er}, 1°, de la loi organique du 30 novembre 1998).

Ces mesures ne peuvent donc pas être utilisées dans le cadre de missions liées à des enquêtes de sécurité, à la protection de personnalités, à la sécurité militaire et à la protection d'un secret confié au Service général du Renseignement et de la Sécurité. Il importera, dès lors, d'établir suffisamment de mesures de protection internes afin de garantir le strict respect de la finalité de cette collecte de données.

La requête adressée à l'opérateur de télécommunication ou au fournisseur d'un service de télécommunication peut émaner du dirigeant du service ou de son délégué et doit être écrite et motivée.

En cas "d'extrême urgence", les officiers des services de renseignement et de sécurité peuvent, par une décision écrite et motivée et avec l'accord oral préalable du dirigeant de leur service ou de son délégué, requérir ces données en temps réel. Cette décision doit être communiquée au dirigeant du service dans les 24 heures.

Cet article s'inspire de l'article 46bis du Code d'Instruction criminelle (loi du 10 juin 1998).

6. S'il peut être souscrit aux motifs d'extrême urgence, la Commission estime néanmoins justifié de demander des garanties supplémentaires compte tenu du large champ d'application de ces enquêtes et du climat sensible dans lequel elles ont lieu. Elle recommande, dès lors, que :

- 1) la requête écrite fasse explicitement mention de l'accord oral préalable (qui, quand...) afin de permettre un contrôle a posteriori;
- 2) la communication des données par l'opérateur ou le fournisseur de service, y compris lorsqu'elle est requise par des officiers, soit obligatoirement faite au dirigeant du service ou à son délégué.

Ces derniers assument une responsabilité finale manifeste, y compris donc en ce qui concerne les questions relatives au respect de la vie privée.

Dans le texte néerlandais, le terme "gedelegeerde" doit, selon la Commission, être remplacé par le terme "gemachtigde".

En outre, la Commission souhaite être consultée au sujet du projet d'arrêté d'exécution prévu à l'article 3, § 3, in fine.

7. L'article 4 porte sur les mesures de repérage et de localisation, à savoir la technique dite du "Zoller-malicieux" qui permet d'enregistrer des numéros d'appel de et vers un appareil ainsi que la localisation de l'origine et de la destination d'une télécommunication et la communication des factures relatives aux données d'appel. Inspirée de l'article 88 bis du Code d'Instruction criminelle (art. 5 de la loi du 10 juin 1998), cette disposition est, elle aussi, assortie d'une série de garanties : ces mesures sont exclusivement autorisées dans le cadre de missions de recherche, pour une durée maximum de deux mois (mais prolongeable) et peuvent uniquement être requises par le dirigeant du service ou son délégué (pas par des officiers), par une demande écrite et motivée. La requête ne peut concerner des données en temps réel qu'en cas de nécessité impérieuse mais doit de toute façon être faite par écrit et de façon motivée. L'obligation de collaboration des opérateurs ou fournisseurs de service sera établie par voie d'arrêté royal. A cet égard également la Commission demande à être consultée pour avis. Le refus de collaborer peut, dans ce cas-ci également, entraîner des sanctions pénales. La Commission ne formule pas d'autres observations sur ce point.

8. Le chapitre III traite des mesures de surveillance. La section 1 (art. 5 et 6) en définit le cadre légal et les conditions d'utilisation. En se fondant sur l'article 90 ter, § 1^{er}, du Code d'Instruction criminelle, les services de renseignement et de sécurité peuvent appliquer les méthodes d'investigation particulières d'interception de (télé)communications privées (écoutes de sécurité). En raison du caractère sensible de ces mesures sur le plan du respect de la vie privée, le recours à ces mesures est soumis à des conditions très strictes. Ainsi, l'opération n'est possible que :

- dans le cadre de missions de recherche, d'analyse et de traitement de renseignements sur la base des articles 7, 1^o, et 11, § 1^{er}, 1^o, de la loi organique.
Les enquêtes de sécurité, la protection de personnes et les missions relatives à la sécurité militaire et à la protection d'un secret militaire sont donc à nouveau exclues;
- dans des cas exceptionnels;
- lorsqu'elle est nécessaire et à titre subsidiaire (lorsque les autres mesures de recherche sont insuffisantes);
- pendant la transmission des communications (donc sur le trajet entre l'émetteur et le récepteur). La prise de connaissance du résultat d'une communication (p. ex. la lecture d'un e-mail ou d'un fax mis en mémoire chez le destinataire) est donc interdite;
- lorsqu'il existe des indices sérieux que certains intérêts de l'État ou de la de population sont menacés. Concernant la sûreté de l'État, il s'agit d'activités d'espionnage, de terrorisme, d'extrémisme, de prolifération, d'organisations sectaires nuisibles, d'organisations criminelles et d'ingérence telles que définies à l'article 8, 1^o, de la loi organique (art. 5, § 1^{er}, in fine). Il s'agit, en outre, d'activités menées contre l'intégrité du territoire national, les plans de défense militaires, l'accomplissement des missions des forces armées, la sécurité des ressortissants à l'étranger et d'autres intérêts fondamentaux à définir par le Roi (art. 11, § 2, de la loi organique) (art. 5, § 2);
- lorsqu'elle est dirigée contre des personnes qui sur la base d'indices précis sont soupçonnées de se livrer à de telles activités et des personnes présumées être en communication régulière avec le suspect (art. 5, § 3). Par conséquent, aucune écoute proactive ou exploratoire n'est possible.

L'article 6 rappelle le principe de finalité et limite l'utilisation des données aux fins mentionnées ci-dessus, sans préjudice de l'article 29 du Code d'Instruction criminelle (obligation pour le fonctionnaire d'informer la justice).

La Commission considère que des garanties suffisantes ont été prévues afin de préserver le caractère exceptionnel de ces mesures, sous réserve toutefois des modalités d'exécution, lesquelles doivent assurer une protection optimale de la vie privée (cf. infra).

9. En ce qui concerne l'exécution des mesures, l'article 7 prévoit qu'une écoute de sécurité nécessite l'autorisation préalable du ministre compétent, sur proposition du dirigeant du service. Cette garantie accrue est assurément justifiée vu le risque très élevé de violation de la vie privée du citoyen que peut représenter cette mesure d'écoute. L'article 7, § 2, précise que l'autorisation doit être écrite et datée et doit obligatoirement mentionner :

- les faits ou indices concrets;
- le caractère indispensable de la mesure;
- la personne, le lieu ou les moyen soumis à surveillance;
- la période (max. 3 mois);
- l'identification des officiers commis pour l'exécution.

Si la Commission approuve ces conditions, elle estime toutefois que l'autorisation écrite doit être clairement motivée afin de faire ressortir manifestement le caractère subsidiaire d'une telle mesure. Actuellement, cette condition n'est prévue qu'à l'article 8 en cas de prolongation ou de renouvellement.

La prolongation et le renouvellement sont soumis aux mêmes conditions formelles que la première autorisation. La prolongation, motivée, peut être autorisée au maximum six fois, chaque fois pour une durée de trois mois.

Ensuite, seul un renouvellement peut être obtenu si l'existence de "circonstances précises nouvelles" est démontrée.

La Commission ne formule aucune remarque à cet égard.

10. L'article 9 impose aux opérateurs ou fournisseurs de service de prêter leur concours technique si le ministre en fait la demande et prévoit la possibilité d'infliger des sanctions pénales en cas de refus.

11. L'article 10 règle les modalités d'enregistrement et de transcription des écoutes ainsi que leur conservation et leur traduction éventuelle. L'objet de la mesure, les jours et heures auxquels elle a été exécutée sont enregistrés au début et à la fin de chaque enregistrement. Seuls les enregistrements jugés pertinents pour les missions visées aux articles 7, 1^o, et 11, § 1^{er}, 1^o, de la loi organique font l'objet d'une transcription. Les notes prises dans le cadre de l'exécution de mesures prévues à l'article 5 du projet ne peuvent être utilisées que si elles sont consignées dans un rapport. Dans le cas contraire, elles sont détruites.

Les enregistrements et transcriptions de communications jugées pertinentes (accompagnés éventuellement d'une traduction) sont conservés dans un lieu sûr désigné par le dirigeant du service.

La Commission estime que – outre la conservation de toutes les communications ayant fait l'objet d'écoutes – les conversations non pertinentes doivent figurer de façon sommaire dans la transcription. La pertinence d'une conversation peut être appréciée différemment par les services de renseignement et de sécurité et par les suspects. Cela peut – dans le cadre d'une affaire judiciaire ultérieure – profiter aux droits de la défense.

La Commission souligne l'importance d'un délai de conservation. Le § 6 de l'article 10 laisse à un arrêté royal le soin d'en définir les modalités. La Commission demande expressément à pouvoir émettre en temps opportun un avis sur cette question.

Le rapport au Roi du présent projet de loi précise que la réglementation proposée est largement inspirée des dispositions pertinentes du Code pénal et qu'elle est en phase avec celles-ci.

L'article 90sexies du Code d'Instruction criminelle prévoit que "les enregistrements ... accompagnés de la transcription des communications ... estimées pertinentes pour l'instruction par l'officier ... commis ... sont transmis au juge d'instruction..."

L'alinéa 2 dispose que : "...le juge apprécie quelles sont, parmi toutes les informations, communications, ... recueillies, celles qui sont pertinentes pour l'instruction. Dans la mesure où ces informations, ... n'ont pas été transcrites ..., elles seront transcrites et traduites à titre additionnel."

L'article 90sexies détermine ensuite la procédure de conservation et de destruction de toutes les pièces pertinentes.

Il découle des dispositions de l'article 90sexies que les parties pertinentes des communications enregistrées doivent être transcrites. Cette transcription constitue une garantie supplémentaire pour l'intéressé.

Il serait dès lors logique d'inclure dans le présent projet une disposition similaire qui prévoit la transcription obligatoire des points pertinents et qui ne se limite pas à la possibilité de procéder à une transcription. La Commission recommande que les dispositions du Code pénal soient reproduites dans le projet.

La consignation de toutes les mesures de surveillance, y compris de leur destruction (art. 10, § 5), dans un registre spécifique est une garantie de transparence supplémentaire. La Commission ne formule aucune remarque à cet égard.

12. La centralisation des mesures de surveillance sera organisée par le Roi (art. 11). A cet égard, les mesures en matière d'écoutes judiciaires peuvent servir de modèle (voir également l'avis 01/2001). La Commission souhaite être consultée au sujet du projet d'arrêté royal.

13. La section 4 contient diverses dispositions. L'article 14 prévoit que le Comité permanent R est informé sans délai de toutes les mesures, ce qui permet de procéder à un contrôle – bien que celui-ci se fasse a posteriori.

La Commission rappelle une fois encore que cette disposition ne porte en rien préjudice aux compétences que lui confère la loi du 8 décembre 1992 en matière de contrôle (art.13).

14. Au chapitre IV, l'article 15 prévoit l'applicabilité de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, ce qui permet d'entourer les mesures, les informations obtenues par celles-ci et les modalités mises en œuvre pour les obtenir de toute une série de mesures de protection. L'article impose ensuite une obligation de secret aux personnes qui apportent leur concours dans le cadre de cette loi. L'article 16 détermine les sanctions en cas de violation de cette obligation.

15. Enfin, l'article 17 impose à chaque Ministre concerné l'obligation de faire annuellement rapport au Sénat.

PAR CES MOTIFS,

la Commission émet un avis favorable sous réserve des remarques formulées.

Pour le secrétaire,
légitimement empêché :

Le président,

(sé) J. VANSEVENANT,
conseiller adjoint.

(sé) P. THOMAS.